August 1994/Number2-94

security awareness bulletin

Information Systems Security

Defining the Threat to Information Systems 1
The Boeing Hacker Incident 19
Center for Information Systems Security 25

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Security Education and Awareness Team, 8000 Jefferson Davis Hwy, Bldg 33E, Richmond VA 23297-5091; (804) 279-5314, DSN 695-5314. Fax: (804) 279-5239 or DSN 695-5239. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods .

New distribution, address changes:

Government agencies: DoD Security Institute, 8000 Jefferson Davis Hwy, Richmond VA 23297-5091, POC Del Carrell, (804) 279-5314, DSN 695-5314; fax (804) 279-6406, DSN 695-6406

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria VA 22314-1651

DISP contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Without the basics, you're just not building . . .

Enroll Now in DoDSI's New

Basic Information Security Independent Study Course

Includes 4 subcourses:
Classification Management (Part 1 & 2) (DS3101/3102)
Protecting Classified Information (Part 1 & 2) (DS3103/3104)

To enroll, send DA Form 145 to:

Army Institute for Professional Development
U.S. Army Training Support Center
Newport News, VA 23638-0001

Information Systems Security: A Note to Security Educators

The role of the security educator as proponent of security awareness in a work-place environment that includes advanced automated systems is constantly expanding. As we come to depend more and more on electronic storage, processing, and transmission of information, members of our employee populations, without exception, must be informed about the unique threats and security safeguards that apply to the modern workplace.

The two feature articles that appear in this issue of the Bulletin have been selected because they offer useful ideas and factual information that you might include in a security educational program. The first of these, "Defining the Threat to Information Systems," could serve as the basis for a briefing or newsletter feature on this subject. In either form, of course, it should be edited, supplemented, and otherwise "tailored" to meet the needs of your organization.

Both articles originated as presentations to the Conference on Computer Crime: A Peopleware Problem, held at the Defense Personnel Security Research Center, Monterey, California, in October, 1993. And they also appear in the proceedings of that conference.

Defining the Threat to Information Systems:

A Challenge for Security Educators

by Lynn F. Fischer
Department of Defense Security Institute

The common use of automated information systems components in the modern workplace in both government and industry and the continued need to protect information from competing interests at both the national and corporate level has made necessary (1) the application of new security countermeasures for automated systems, and (2) additional security education for personnel having access to these systems. Both advanced countermeasures and enhanced security education are based on the belief that there is a persistent "threat" from either external or internal sources—a threat which often lacks clear definition in terms of (a) what exactly is being threatened, (b) why it is being threatened, (c) where the threat is coming from, (d) how might it be carried out, and (e) what we are supposed to be doing to prevent it?

Sound familiar? These are the classic questions addressed by security educators everywhere, in automated and non-automated environments alike. And among the historic objectives of security awareness programs in government aimed at the protection of classified and sensitive information is our task of providing credible answers to these questions. In fact, for the government security educator, never has the need to define a credible external threat been so urgent as now, following the collapse of the Soviet Empire and the dismemberment of communist regimes. We are constantly challenged by cleared personnel to explain why, since the KGB is no more, we still need an array of elaborate protective measures.

Developing a Strategy for INFOSEC Awareness

Therefore the central purpose of this article is to map out what might be an appropriate strategy for a security educator (perhaps like yourself) confronted with the new challenge of giving a "computer security briefing" or, more properly stated, educating employees in information systems security. Before attempting to do this, I must ask the reader to consider two predictions about the future of our professional role regarding security awareness. These serve as stepping off points for what follows.

One prediction is that educational activities related to information systems security in the future will be carried out by a *generalist* security professional who does not have unique or technical qualifications in automated information systems, computer science, or electrical engineering. Just as paper and film as media for communication have been taken for granted in the past, so it is that in the modern workplace, moving into the 21st century, the use of electronic media and computer processing of information will be universally accepted features of our work.

A second forecast is that information security in any type of environment will remain essentially a human issue. For example, we can spend millions on NSA endorsed "trusted systems," but if the people who have access to those systems are not trustworthy (loyal, reliable, and aware), it's all for nothing. The same could be said if they don't know when or how to apply a specific technical security countermeasure.

One implication of these two assumptions about the future is that we as security educators are now, or will be, all in the same boat—sharing reponsibilities for training and awareness of personnel in the modern automated workplace, and that the protection of information, whether digitially recorded on magnetic media or on steno pads, is a people problem.

Four messages we need to communicate

Perhaps the most difficult aspect of this new educational challenge is how to approach the job: what is important to include (and not to include) in a training or awareness program, and how to organize that material. What follows is, in my opinion, some good advice about the central arguments that we need to get across to an often-times skeptical audience.*

**For many of these ideas we are indebted to security educators such as Joseph Grau at the Department of Defense Security Institute, and more recently by Captain John McCumber of the Defense Information Systems Agency who has written extensively on informations systems security.*

1. "Information systems security" is no more than information security for the modern workplace. We are building on long-established principles, policies, and practices.

The conceptual distinction between conventional information security and "information systems security" is fast becoming artificial. At best it has been a convenient way to organize the work of security professionals. At its worst, it perpetuates the myth that security countermeasures in an automated environment is too technical for just anybody to understand. However, what has been good advice to security educators for years in non-automated environments is generally still valid. But the same principles may have to be described with new terminology, and remedies prescribed in the form of new and somewhat different countermeasures.

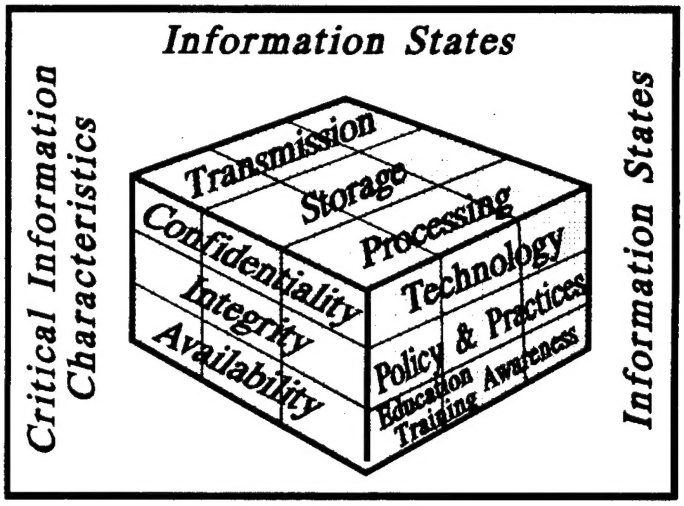
Not everybody in the security profession is happy about this idea. At the 1993 Department of Defense Security Conference, heated and anguished objections were raised by many senior security officers about discussing AIS/computer security as "INFOSEC." Whichever way we may slice up the policy or distribute the procedural duties in the security world, the fact remains that the above proposition can make sense to the rank and file employees if logically explained. Furthermore, if we can successfully sell the idea, this will go a long way to demythicize security countermeasures for automated systems and electronic processing. And as a result, our personnel will begin to see information systems security as more of a human issue and something they are empowered to support, rather than as too technical to understand.

Getting a view of the Big Picture

How can we achieve this educational objective? There are no easy answers. But of particular value, not only for organizing our own thinking but possibly as an instructional device itself, is the three-dimensional INFOSEC Model described by Air Force Captain John McCumber in his September, 1991, *Security Awareness Bulletin* article, "Security Measures for the State-of-the-Art Workplace."

This model as outlined can be applied to the conventional workplace as well as to a fully automated environment. McCumber explains that information in any of three states (transmission, storage, or processing) is subject to three types of threat (to its confidentiality, integrity, and its availability to a legitimate user). The threat, if succcessfully carried out by an adversary, might result in the theft, corruption, or destruction and/or denial of access to a legitimate user.

McCumber's third dimension categorizes security countermeasures appropriate for each state and each critical characteristic. The countermeasures also have



three categories: technology, policy & practice, and education. What we end up with is a three-dimensional map, as shown below, for evaluating the security effectiveness of any information system. The resulting 27 cells can be evaluated independently, each with its own appropriate security countermeasures.

While useful to an analyst engaged in system certification (which apparently was McCumber's original intent), one might hesitate to employ this diagram as an instructional aid for a typical audience or readership. At first glance, it looks complicated, and it is somewhat at odds with the best advice of seasoned trainers: The KISS Principle ("keep it simple stupid" or you lose your audience). And there *are* simpler variations of this model that have potential for security education. In the same 1991 *Bulletin* article, McCumber offers a table showing three categories of countermeasures in which countermeasures are identified for each of three states of information. This, in my opinion, does have potential as a way to get people thinking about how they can protect information in an automated environment.

But more importantly, this framework provides the opportunity for comparing security countermeasures of all types including the traditional world of paper, padlocks, inkpads and file cabinets. Only a sampling of the total inventory of countermeasures for the workplace is listed above. It might be possible, as an interesting instructional exercise, or as part of a security briefing, to identify comparable security procedures and measures for a non-automated environment for each countermeasure appropriate for information systems security.

Layers of Security Measures by Information States

	TRANSMISSION	STORAGE	PROCESSING
TECHNOLOGY	STU-III Data encryption devices Code Parity error checks	Access codes Password controls Physical safeguards Intrusion protection SCIF construction	Trusted systems (NSA) User recognition systems Multi-level processing Error traps Anti-virus software
POLICY/ PRACTICE	Data encryption standards Personnel security	User access policy User authorization Approved systems (DIS) Physical safeguards Approved storage Personnel security	Access control policy Approved systems (DIS) Audit trails Personnel security
EDUCATION TRAINING AWARENESS	COMSEC training STU-III indoctrination	Security indoctrination Physical protection training	Security indoctrination Security education Computer security briefings

Probably the logical conclusion to this exercise would be for the security educator to reaffirm the basic principles of information security such as need-to-know, accountability, control of access, physical protection, personal safeguarding, and employee responsibility for reporting. As new technologies for the transmission, storage and processing of information emerge, we simply add new and technologically appropriate countermeasures to the inventory.

2. Severe damage to government and defense-related information by both internal and external offenders has occurred in the very recent past. It can happen to any organization, and the damage can be significant.

It is not easy to find reliable case studies material for use in briefings or awareness publications without a systematic coverage of news sources. But unless we can show that the lack of adequate security has real and tangible consequences, our programs will lack credibility in the minds of our target audiences. On the following two pages is a rough attempt to list the more important criminal cases or events which have affected defense-related information systems since 1987. Included here are only those events which have come to public knowledge through media coverage with a few notes on systems penetrated, damage or compromise, and possible motivations. Behind each entry is a potentially interesting case study that might be fleshed out with additional research. Most, but not all, of these events are related to computer hacking—defined in the 1990s as illegal or unauthorized access to a system or network using telephonic communication from a remote site.

The use of case information in security education is a long and honored tradition which most of us believe is extremely effective if handled correctly. We have seen in the past that one of the best ways to capture the attention of an audience is to tell them stories, particularly stories about the sins and failings of people just like themselves — perhaps for the same reasons people love soap operas. Nevertheless, these stories work and they serve as vehicles for several teaching objectives.

The discussion of classic espionage cases in security awareness briefings and video products brings the foreign intelligence threat and the act of espionage into the world of reality. Furthermore, by showing the extensive damage to national security resulting from each betrayal, our employees are (we hope) more willing to see security countermeasures as being important and worth implementing since they may even save lives.

Principal Cases of Computer Crime Impacting on Defense-related and U.S. Government Information Systems*

Name (Age)	Date	Systems Penetrated/Compromised	Damage/Compromise	Stated Motivation
Herbert Zinn (17) (Shadow Hawk)	1987	Bell Laboratories US Missile Command System Robbins Air Force Base	Software theft valued at $1.2 million artificial intelligence advance computer design	-
West German Hackers	1986-1989	Lawrence Berkley Labs Pentagon systems Los Alamos National Labs NASA	Extensive loss of sensitive data	Money (KGB operation)
Robert Tappan Morris	late 1988	INTERNET nationwide network affecting Lawrence Livermore Labs, Army Ballistic Research Lab, & NASA Ames Research Center	Infected network with virus (worm) shut down network of 6,000 UNIX- based computers	Intellectual challenge out of control
Michael Peri	Feb 1989	(U.S. Army, W. Germany)	Passed classified media to East German Intelligence	Frustration at work
Legion of Doom Internet break-in	Jun 1989	AT&T switching computers	Planted time bombs; Damage $1 million	Hope of financial gain
Levittown Hacker (15)	Sep 1989	Grumman VAX system	Military-related databases & programs	-
MOD (Masters of Doom) led by Zod (14) (13 hackers arrested)	Nov 1989	Secretary of the Air Force	Crashed the system $250,000 to repair sensitive information compromised	-
Richard George Whitman (24)	Mar-Jun 1990	NASA Marshall Space Center Goddard Space Flight Center	Altered/damaged data	-
Michael Lauffenburger	Mar 1990	General Dynamics Space Division	Planted logic bomb in Atlas Missile parts program	Revenge Lack of recognition
Leonard Rose Jr. (32) (former member of Legion of Doom)	May 1990	AT&T Unix Software	Trojan Horse in software for access to AT&T	-

Name (Age)	Date	Systems Penetrated/Compromised	Damage/Compromise	Stated Motivation
Masters of Deception Mark Abene (20) aka Phiber Optik four other NY youths (all 22 or younger)	1990-1992	Southwestern Bell Martin Marietta IT&T TRW Pacific Telesis Group	$370,00 loss by S.W. Bell; stole passwords, credit information; destroyed data	To enhance image gain prestige, intimidate other hackers
Dutch Teen Hackers	Apr 1990- May 1991	Kennedy Space Center Pacific Fleet Command Lawrence Livermore Labs Army, Navy, A.F. (34 sites)	Obtained highly sensitive files on U.S. war operations; modified or copied data	-
Australian Hackers Nahshon Even-Chaim (18) Richard Jones (20) David Woodcock (21)	Feb 1990	NASA, Norfolk Lawrence Livermore Labs US Naval Research Lab. through Internet System	Loss of NASA system for 24 hours; deletions, alteration of data	Boost to self-esteem renoun enjoyed thrills
Kevin Lee Poulsen (17) (Dark Dante)	1983-1992	Army MASNET, DoD ARPANET, Ft. Bragg, SRI, Rand Corp.	Charged with espionage; obtained classified document	Driven by ego
Ronald Austin (19)	1983	Pacific Bell Telephone	Federal wire taps compromised	Money, need for recognition
Charles Anderson (19) Costa G. Katsaniotis (21)	Oct 1992	Boeing Aircraft Environmental Protection Agency	Illegal access to UNIX system; copied passwords	
Danish Hackers four arrested (17-23)	Dec 1993	NOAA computer network; 32 systems in U.S.	Illegal access; copied password files	

* This listing is based on a database search of public media reports from 1987 to the present; the author does not suggest that it is necessarily complete.

Thus by adopting the strategy of a traditional security educator who wants to make "the threat" credible by talking about real offenders, and by a regular exploitation of media sources and official reports, we can put a human face on computer crime. We can discuss, for example, the type of people who might attempt to sabotage a system with a Trojan horse or virus. We can get an idea about what motivates some teenagers to create havoc in some of the most extensive research networks in the nation.

As in the classic espionage cases, each of these computer crime stories offers lessons learned. However, one big difference between the two categories of events is that while in almost all of the recent classic espionage cases (John Walker, Thomas Cavanagh, William Bell, James Hall, Larry Wu Tai Chin) betrayal of public trust is a common denominator, this is much less typical of computer crime cases endangering national security where the perpetrator was never authorized access to the system into which he intruded. There are two or three inside-jobs listed here, but in most of these events the crime is "breaking and entering" by a total outsider who can do enormous damage from a remote location.

3. Foreign intelligence services represent only one of several sources of threat to our systems. We have to address both external and internal threats.

Referring again to one of the eternal questions that each security educator is duty bound to answer, "Where is the threat coming from?" we can see here another contrast between classic espionage and contemporary computer crime. Whereas the former events nearly always involve foreign interests and foreign intelligence services at some point in the activity, computer crime endangering national security rarely is associated with a foreign intelligence organization, at least among cases that are openly acknowledged. But this may be illusory; it is quite conceivable that the penetration of sensitive government and defense contractor systems by foreign intelligence services is routinely so successful that it goes unnoticed or is not openly admitted.

In 1986 press reports announced the probable exploitation of unclassified but sensitive U.S. defense-related data through a Vienna-based research institute which employed both Western and Soviet Bloc scientists. This was done by conventional long-distance telephone and with legitimate access procedures.

The only publicly known instance of foreign intelligence involvement in a hacking scheme was seen in the case of the West German Hackers who served as a conduit for sensitive U.S. Government information going to the KGB. The full account of this story is found in Clifford Stoll's entertaining book, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. In an entirely different category is the case of Michael Peri, who physically delivered classified floppy disks and a computer with a classified file on the hard drive to East German Intelligence in 1989. Of the other offenders listed here, only Kevin Lee Poulsen was charged under the espionage code for having illegally obtained a classified document (presumably by electronic transmission). This was reported to have been an Air Force Tasking Order, containing flight orders for Army paratroopers on a 1987 military exercise at Fort Bragg, N.C.

In most of the events that involve the penetration of a national-level information system, what we do see reported, however, is an act committed not by a representative of foreign interests but by a very young individual whose motives are not clear and who may have no real interest in providing illegally accessed information to any foreign interest. In many of these situations it turned out that the greatest threat to the information posed by hackers was not so much in its being compromised, but in its being altered, destroyed, or denied to legitimate users.

One can see in the cases listed here the predominance of a "domestic" threat (with a few foreign penetrators) acting on behalf of no one else. But in most cases, the offenders operate from outside of a restricted access system. In a larger number of computer crime cases in which private sector systems and data are targeted for illegal profit (not included in the listing), the culprit is typically an "insider;" that is, a person like logic bomber Michael Lauffenberger who had authorized access to the system, if not to all of the information contained in that system. These are some of the significant differences and similarities between what might be called the conventional or traditional threat to protected information by foreign intelligence services on one hand and the emerging threat to information systems on the other.

Motivation: why do they do it?

While governmental and independent organizations report annually on the enormous cost to private sector firms from computer crime apparently committed for financial gain,[§] those who attack and penetrate government and defense community systems may be driven by

far more complex motives. At this point in time, suggestions about the underlying motivations of Herbert Zinn, Mark Abene, the Dutch or Australian Hackers, Kevin Poulsen, and others is guesswork. However, press reports mention such things as intellectual challenge, thrill, ego satisfaction, a craving for recognition and prestige, and the boosting of self-esteem as driving forces.

John Markoff, writing in the *New York Times* quotes one unnamed researcher at a Silicon Valley research institution as concluding that these hackers have an anti-social obsession. In recent years the researcher offered four underground hackers salaried programming jobs in an effort to channel their energy away from the destructive use of computers. In each case the experiment failed:

> "They're misfits, losers or troubled individuals lacking a sense of duty or morals ... Every single one of them had deep psychological problems."

To better examine the predisposition to this category of crime, the Community Research Center, a group of Federal agency clinical psychologists, has initiated a study of the psychological make-up of computer offenders. This, like CRC's ongoing research on espionage felons (Project Slammer), will be based on in-depth, interviews with each offender under clinical conditions.

What can be said to our employee populations about the reality of the external threat to information systems?

With the help of counterintelligence professionals in the FBI, DIA and other agencies, we are beginning to put together a response to this question that is both believable to our employee populations and factually accurate. Without going into unnecessary detail, the facts are these: While the KGB in name is gone, the GRU remains active and the post-Soviet Russians still target critical defense-related information. The foreign intelligence threat is coming at us from diverse sources—friend and foe alike. This includes organizational entities which are not nation-states: international corporations, terrorist groups, rebel factions, and organized crime. High on the list of targeted information is advanced technology having military application which may or may not be formally classified. Lastly, we know that our economic competitors overseas work very closely with their respective national intelligence organizations to acquire our protected technologies. And there is no reason to believe that these intelligence services have failed to take advantage of human talents and new technologies that can be mobilized to penetrate our information systems.

This recent redefinition of the foreign intelligence threat for the 1990s and beyond is relevant to the issue of information systems security since it broadens the range of possible non-domestic sources about which we must be alert. But for the security educator who is tasked with the job of briefing and in other ways educating co-workers, supervisors, and executives functioning in an automated workplace, this is only part of the answer, and as discussed above, the source of the threat is only one of the several awareness issues that must be addressed.

4. We are not helpless when confronting these potential threats to automated systems. There are things that every employee can do to minimize the risk of compromise or loss of information.

Having informed people of the reality of a threat, we then need to tell them what they can do about it. This is always one of the themes (or should be) of an effective security awareness communication to employee populations whose members have the responsibility for safeguarding classified or sensitive information. Regrettably some security educators don't construct for their audiences the link between the threat to information and the application of specific security countermeasures. Another frequently missing element in security education is specific information about past damage from security failures and potential consequences of future disasters. All the more reason to review past crime and espionage cases where the damage can be spelled out in dollars or military consequences.

Experienced security educators tell us that our employees *will* pay attention to security briefings if they are provided with specific information that is concretely related to their day-to-day tasks and to their professional success. What follows is a plan for discussing on-the-

---

§The FBI's White-Collar Crime Section reported in 1993 that their caseload for computer crime has quadrupled in the last two years. The Council of Better Business Bureaus reports that U.S. businesses lose $3 billion to $5 billion annually to computer crime.

Threats and Security Countermeasures for Informations Systems

Critical Characteristics of Information Subject to Threat	Modus Operandi or Criminal Action	Security Countermeasures
1. Confidentiality	Hacking from remote location Unauthorized access Insider theft of media Illegal sale of data/software Espionage by employee Electronic eavesdropping Theft of passwords	Effective access codes Password controls Personnel security measures Security education Data encryption Multi-level processing Approved systems
2. Integrity	Hacking from remote location Insider sabotage Introduction of virus Alteration/deletion of data	Effective access codes Password controls Personnel security measures Anti-virus software Audit trails Physical security
3. Availability	Introduction of worm to network Insider sabotage Insertion of logic bomb, trojan horse, virus, bacteria	Access controls Anti-virus software Audit trails Personnel security measures

job employee responsibility for information systems security. In this table, specific ways in which insider or external offenders threaten information are grouped according to which of three critical characteristics of information they endanger: confidentiality, integrity or availability. To the right are safeguards and methods available to personnel for use in preventing or counteracting specific threats. For example, the probability of success by a remote hacker would be minimized by effective access controls. Insider sabotage might be precluded by effective personnel security and a continuing evaluation program that deals with employee dissatisfaction before it gets out of hand.

The final message to convey to the audience by the security educator is that good security depends upon everyone's involvement and support in the process and that security professionals are there to help, advise and assist, rather that to apprehend or catch the slacker.

In summary, the probability of success in selling the above four arguments to employee populations will be greatly enhanced by fully integrating security education for information systems into the comprehensive programs for security education. Partitioning out "computer security" as an esoteric specialization automatically creates a barrier to rank and file employee involvement and understanding. Furthermore, much depends upon the educator's ability to accurately define the threat to information systems drawing on current and authoritative counterintelligence reports and up-to-date case information from media reports and other sources. Experience has shown that what our personnel pay attention to is not abstract generalizations, but real facts about real people and events having consequences or payoffs that everyone can relate to.

Courses from the DoD Security Institute:

Information Systems Security Basics 5220.22

The course provides practice in fundamental computer security skills to support the protection of information and information systems in the Department of Defense. Given modules of instruction, practical exercises, a technical laboratory environment, and a library of reference materials, the student will be able to: Explain the threat to and vulnerabilities of information systems and employ appropriate security countermeasures to manage threat and minimize vulnerabilities; identify required physical, personnel, and procedural security procedures for information systems; and describe the elements of the information systems accreditation process. To enhance their job performance in the workplace, students will be given a "Security Information Technology User's Package" (SITUP), a collection of regulations, references, handbooks, newsletters, training aids, and agency points-of-contact.

Target audience:
Priority 1: DoD personnel assigned or projected for assignment to perform the following information systems support functions for their organization: Preventing, detecting, and eradicating viruses; auditing information systems; evaluating access controls; clearing and purging of media; and evaluating accreditation plans.

Priority 2: Employees of other federal agencies with similar duties and responsibilities may attend the course on a space available basis.

Priority 3: Policy and oversight, inspection and/or audit, and other personnel functioning in support of the INFOSEC mission.

Required personnel security clearance: None

Prerequisites: Students must complete and will be evaluated on their comprehension of reading materials provided to them before class. These materials identify and define information systems technology in order to establish a common computer literacy baseline. Due to course design and time constraints, remedial training is not available.

To register: By invitation only. Nominations are validated through Information Systems Security program managers at component or agency level. Points of contact for registration are:

Air Force	Mark Queener, AFC4A, Scott AFB, IL (618) 256-2586/DSN 576-2586.
Army	Phyllis Bailey, DISC4, Arlington, VA (703) 696-8061/DSN 226-8061.
Navy/USMC	Raymond Dohm, NISE-EAST, Washington, DC (202) 282-0702/DSN 292-0702
DISA	Maria Lewis, DISA/UAI, Ft Richie, MD (301) 878-4678/DSN 277-4678.

For more information on attendance by other DoD agencies/activities or on course content, call Christ Breissinger (804) 279-3174/DSN 695-3174; or Linda Braxton (804) 279-6076/DSN 695-6076. Fax extension is 6155.

Course Dates:
Apr 10-14, 1995
May 15-19, 1995
Jun 12-16, 1995
Jul 10-14, 1995
Aug 14-18, 1995

AIS Security Procedures for Industry 5220.10

The course describes the security requirements to be implemented by Department of Defense (DoD) contractors who process classified information on AIS. The discussion of computer technology fundamentals and the description of system vulnerabilities provide insight as to why certain security procedures are required. The duties of the contractor personnel delegated the AIS security responsibility are highlighted. The process for requesting written accreditation prior to processing classified information is addressed including a description of the security plans and procedures which must be written. The security modes of operation are described and the types of system events that must be documented are identified. Additional requirements discussed include those pertaining to physical security, software controls, media handling and disposition, maintenance, audit records, and network security. During a practical exercise, students review the security plan for a microcomputer and conduct a self-inspection of the system to assess its compliance.

Target audience: U.S. contractor Facility Security Officers (FSOs), Information Systems Security Representatives (ISSRs), Security Custodians (SCs), or individuals whose responsibilities within their companies include overall security, AIS security for the FSO, or AIS security for the ISSR. Department of Defense civilian and military personnel performing in similar positions are permitted to attend on a space available basis.

Required personnel security clearance: None

Locations:

Apr 9-12, 1996	Orlando, FL	Jun 25-28, 1996	Scottsdale, AZ	Aug 20-23, 1996	Los Angeles, CA
May 7-10, 1996	Minneapolis, MN	Jul 23-26, 1996	Washington, DC	Sep 10-13, 1996	Cherry Hill, NJ
Jun 4-7, 1996	San Francisco	Aug 13-16, 1996	Ft Walton Bch, FL	Sep 17-20, 1996	Detroit, MI

Prerequisites: Must read the *Basics Booklet for Information Systems Security.*

To register: Forward nominations to the DIS regional cognizant security office hosting the course, or call any of the following regional offices for information concerning the sessions:

Mid Atlantic Sector, Cherry Hill, NJ (609) 482-6509 x230
New England Sector, Boston, MA (617) 451-4918
Capital Area, Alexandria, VA (703) 325-9634
Southeast Region, Smyrna, GA (404) 432-0826
Southwest Sector, Dallas, TX (214) 717-0888
Midwest Sector, Chicago, IL (312) 886-7737
Pacific Region, Long Beach, CA (310) 595-7666

When this course is taught in residence at DoDSI, you may enroll either by using the Student Information and Registration Network (SIRN) or submitting the enclosed Registration Form.

For more information on course content: Call Delmar Kerr/Christ Breissinger, (804) 279-5309/3174, DSN 695-5309/3174.

DoD Security Institute
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, Virginia 23297-5091

Registration Form

Use this form only if you don't have access to the SIRN. Please print or type, and fill in all *applicable* information. In addition to serving as a permanent record of your registration, a class roster will be compiled prior to class from the information on this form. If you have questions, call the Registrar (804) 279-4891, DSN 695-4891.

Privacy Act Statement

Authority: 5 USC 301 and DoD Directive 5105.42.

Principal Purpose or Purposes: The primary purpose served by DSI Form 2021A is to serve as a permanent enrollment record. Social security number (SSN) is required to distinguish between records of students with the same name.

Routine Uses: DSI Form 2021A is routinely used as an alphabetical index and locator card for students and as a course completion record.

Disclosure: Disclosure of information, including SSN, is voluntary. Failure to provide such information could result in inaccurate records of students with same name.

Course title | Course No. | Course dates

SSN | Name (Last) (First) (MI) (subtitle: Jr., III, etc.)

Position | Mil/GS Grade

Agency/Activity Code (see reverse for codes) | Birth date MM/DD/YY | Sex (circle) F M | Clearance level (circle) C S TS None

Duty station/Facility address | Job Title/Name/Address of Supervisor (if same address ☐)

(city) (state) (zip)

DSN _____ ☐ release authorized DSN _____

Commercial No. _____ Commercial No. _____

Education level | Last college date MM/DD/YY | Years in security field | Years as adjudicator

DoDSI supports the Americans with Disabilities Act of 1990. Attendees with special needs should indicate those needs here, or call (804) 279-4891, DSN 695-4891.

Attendance approved by official? (if identified in the course description sheet) Yes No

FSO Program Management course completed _____ month/year

Personnel Security Adjudications course completed _____ (or Basic Equiv. Test) month/year

DSI Form 2021A/Jan 95

Agency/Activity Codes

Department of Defense

DAF	Air Force
DAY	Army
DAA	Defense Contract Audit Agency
DIO	Defense Information Services Organization
DSA	Defense Information Systems Agency
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DLA	Defense Logistics Agency
DMA	Defense Mapping Agency
DNA	Defense Nuclear Agency
DCR	Directorate for Industrial Security Clearance Review
DJS	Joint Chiefs of Staff
DJT	Joint Command
DMC	Marine Corps
DNS	National Security Agency
DNY	Navy
DSD	Secretary of Defense
DoD	Other Department of Defense

Other Government

AID	Agency for International Development
OAG	Agriculture Department
OCM	Commerce Department
OED	Education Department
OEG	Energy Department
OEP	Environmental Protection Agency
OFE	Federal Emergency Management Agency
OFG	Foreign Government
OGA	General Accounting Office
OGS	General Services Administration
OHS	Health and Human Services Department
OIN	Interior Department
OIC	Intelligence Community
OJU	Justice Department
OLA	Labor Department
OLC	Library of Congress
ONA	National Aeronautics and Space Administration
OSF	National Science Foundation
OTO	North Atlantic Treaty Organization
ONR	Nuclear Regulatory Commission
OPM	Office of Personnel Management
OSB	Small Business Administration
OST	State Department
OTP	Transportation Department
OTR	Treasury Department
OAC	U.S. Arms Control and Disarmament Agency
OCP	U.S. Capitol Police
OIA	U.S. Information Agency
OPS	U.S. Postal Service
OSS	U.S. Senate/House of Representatives
OVA	Veterans Affairs Department
SPB	Security Policy Board

Private Industry

IND	Private Industry

The Security Awareness and Education Subcommittee proudly announces the release of a new video:

As Others See You

Understanding and Reporting Foreign Intelligence Threats

Designed with the scientist in mind — and those in the technical community who safeguard critical technologies, sensitive proprietary data, and government classified information. This video shows that the loss of this information can weaken our national security and dull our economic edge.

In this dramatization, we meet Dr. Woolrich, staff scientist from a U.S. Government laboratory, who is confronted by five foreign admirers, each in a different professional role. Any one of them, despite their credentials, could in reality be a foreign agent or an undercover source for a foreign intelligence service. Which one, if any, is the agent? The audience can learn an important lesson from this fictional scientist, especially if they later find themselves approached by a foreign representative.

Produced for the SAES by the Department of Energy's Office of Counterintelligence, with the assistance of Federal agencies represented on the subcommittee. Run time: 16 minutes. To obtain a 1/2-inch VHS copy, send a check or money order for $9.95 to:

CopyMaster Video Inc.
P.O. Box 684
Department 15
Villa Park, IL 60181

Allow 2-3 weeks for delivery.

For additional information, phone CopyMaster at (708) 279-1276.

Each copy of the video comes with an 18-page presenter's guide which describes specific objectives for awareness programs designed to prevent the loss of critical technology.

You Can Host These Courses On-site at Your Facility
(Industry or Government)

Security Briefers Course (SBC) 522.13, 2.5 days	Train-the-Trainer Course (TTT) 522.13A, 4.5 days
Purpose: To improve your effectiveness as a security education briefer. You will receive instruction on how to: • prepare a briefing plan; • design and use brieifng aids; • present your briefings in a clear and interesting manner; and • evaluate live briefings. As the "Security" in the course title suggests, the briefings must address security requirements, but this is not the emphasis of the course. The course emphasis is on accomplishing the objectives listed above so that you become more skilled and more comfortable at speaking in front of others.	Purpose: to train you to teach the SBC. This workshop, conducted on the 2 days before a scheduled SBC, prepares you to be an instructor for the SBC. You will receive instruction by DoDSI staff on how to: use the SBC materials; • present selected lessons in the SBC; • facilitate the preparation of briefings; • conduct practice briefing sessions; and • evaluate live briefings. Under DoDSI supervision, you will then spend the next 2.5 days teaching your first SBC.

If you are considering participating in the TTT, it is suggested that you: be responsible for your organization's security briefing program; be an experienced security briefer or a graduate of the SBC; have a need to train others to prepare and present security briefings; and have a working knowledge of security requirements. If you want to learn *how* to brief — choose the SBC.

To host the courses described above, please call Linda Braxton, DoDSI at (804) 279-6076 or DSN 695-6076.

These courses are held in succession. The TTT precedes the SBC.

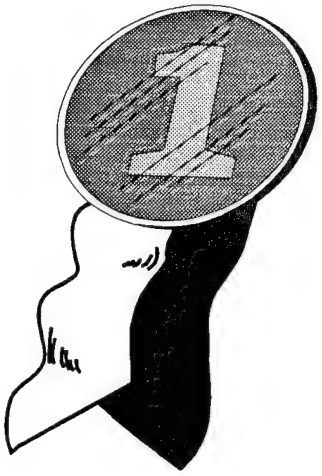
To host the SBC, you must be able to provide:

- ❑ one main classroom for 24 students
- ❑ 3 breakout rooms for 6 students each
- ❑ A-V equipment for all 4 rooms
  (Overhead projectors, screens, and writing surfaces for each room)
- ❑ At least two of the instructors and preferably more for the TTT.
- ❑ An on-site coordinator
- ❑ Invitations to other security organizations in your area in order to fill a class of 24.

The Department of Defense Security Institute (DoDSI) will:

- ✓ Provide the lead instructor and assume responsibility for the teaching success of the course.
- ✓ If necessary, provide security personnel from other organizations to help teach the course.
- ✓ Provide two full days of training for the instructors prior to starting the course.
- ✓ Provide the instructional materials in sufficient quantities for 24 students.
- ✓ Help the trainers teach the Security Briefers Course.

Attention Security Educators, here's your chance to sign up for the:



Train-the-Trainer/Security Briefers Course!

Train-the-Trainer/Security Briefers Course will be offered at the DoD Security Institute in Richmond, Virginia, on these dates

Train-the-Trainer	**Security Briefers Course**
June 3-7, 1996	June 5-7, 1996
September 9-13, 1996	September 11-13, 1996

If interested in attending either of the above classes, please mail us the Registration Form on the last page.

or

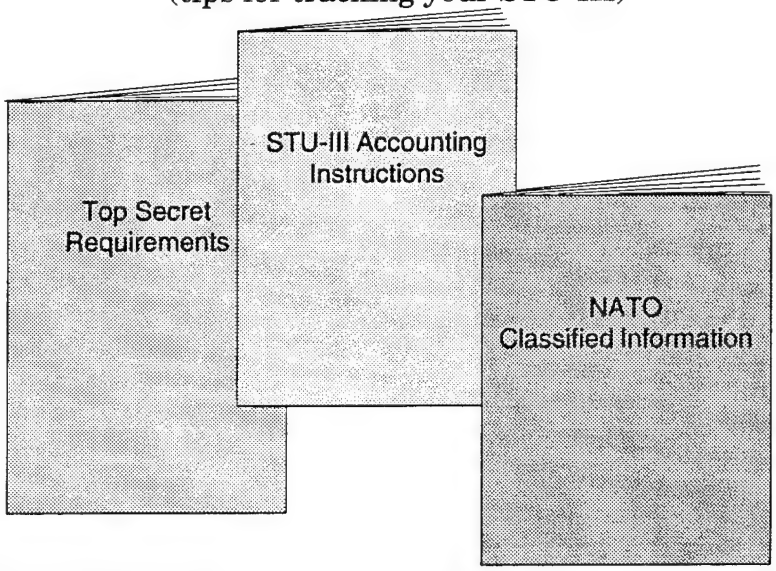
If you'd like to *host* this course, call Linda Braxton at (804) 279-6076, DSN 695-6076.

In addition an on-site Security Briefers Course is being taught:

Dates for SBC:	August 7-9, 1996
Sponsored by:	Security Awareness & Education Subcommittee
Where:	Commerce Department, Washington, DC
Point of contact:	Bob McMenamin
Phone:	(202) 622-1120; FAX (202) 622-1056

3 new job aids for industry!

STU-III Accounting Instructions
(tips for tracking your STU-III)



Top Secret Requirements
(based on the ISM)

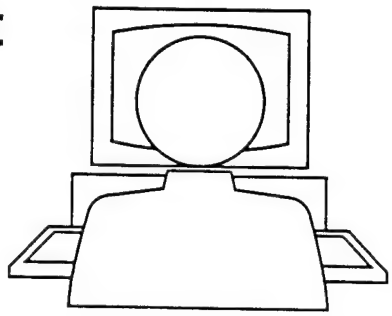
NATO Classified Information
(quick reference guide)

Easy to get ... Easy to use

Contact: DoDSI
Industrial Security Team
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091

or call: (804) 279-5257

The Boeing Hacker Incident



by Rhonda E. MacLean, Senior Manager,
Boeing Computing and Communications Security

Background

With the Cold War behind us, we see an increasing focus on competitive advantage in a global market. This factor is currently influencing the way we do business and will continue to do so for the foreseeable future. Corporations are beginning to recognize the value of intellectual property and its overall contribution to maintaining a competitive edge. At the same time, corporations are using automated systems to further ensure their ability to compete in a world where business transactions are handled in micro seconds versus weeks or months.

Computers and telephones have progressed far beyond boxes on a desk, and are now gateways to business highways. Many corporations are harnessing the latest technology, enabling them unlimited access to world-wide communication networks of data, voice and video. The speed at which technology changes are faced today may pale when compared to the pace of change in the future. It is widely accepted that increased computer usage and computer controlled media will be the "norm" for business transactions.

Protecting those systems and the information contained on them is being reevaluated by many corporations today as a business priority. Unfortunately, in some cases, the shock of having been compromised by an intruder is necessary to gain the corporate commitment to ensure that protective measures are in place and sustained.

Who's using your system?

The Boeing Company received its wake up call in October 1992 when one of its major computer suppliers called and wanted to know why a Boeing account, belonging to a manager who had not used his ID number for several months, was suddenly very active. In reviewing the system logs, it was easy to confirm the user-ID was being used by someone who was not authorized.

By reviewing previous records, we were able to determine the unauthorized activity had been going on for at least a month before the call from the outside supplier. Because the intruders were using an "authorized" account which was not being actively used or monitored by the account owner, the unauthorized activity was not noticed. When the account owner subsequently received his monthly computing charges, he was surprised to see the amount of usage logged by the unauthorized users.

Further investigation revealed the intruders gained access through a conventional modem and off-the-shelf software which made possible rapid sequential dialing that speeded the process. Once the intruders reached a computer, in this case Boeing's computer, the rest was easy. They went on to steal the local area network password files, yielding access to a number of other valid user accounts. Even though passwords are encrypted, password cracking software made easy work of revealing the necessary passwords.

Exacerbating the problem, the violated computer system had established "trusted" network connections with other computer systems inside and outside the Boeing Company. [Once having successfully gained access in one network, a user is assumed to be an authorized user by other networks to which access is sought through the first network.] Taking advantage of this "trust," the intruders were also able to gain unauthorized access to other commercial industry, government agency, and educational systems. We immediately notified those organizations and quickly established an agreement to work with law enforcement to apprehend the offenders.

Monitoring the crime in progress

While we briefed management and developed an internal strategy on the situation, the activities of the intruders were being continuously monitored. The recommendation to allow the intruders to continue unauthorized access while working with law enforcement was approved with the provisions that if any "malicious" activity was detected, we would immediately close the door.

Concurrently, we put together a response team comprised of computing security specialists, technology support persons, and computing security representatives from each operating division. This team met daily to review current activity and to plan the next steps. This team, together with the response processes they developed, would later provide the basis for developing an internal computer emergency response team.

The company Computing & Communications Security Organization took the lead in coordinating the internal activity as well as interfacing with law enforcement agencies. In addition, the company's legal representative was instrumental in assisting the group and in working with law enforcement agencies. We kept the size of the response team to a minimum and each member was advised to maintain confidentiality. The objective was containment while minimizing the risk of "tipping our hands" to the intruders.

Senior managers were briefed daily as to the intruders' activity. Each day management discussed and reviewed the decision to leave the access open or to begin closing the door. In addition, we briefed our senior public relations executive who would have to deal with the news media once the activity became public. This proved to be an important element later in the case.

It's become a Federal case

Although we initially contacted the Federal Bureau of Investigation (FBI), it was unclear which law enforcement agency would actually have authority in this case. We felt confident that both state and federal computer trespass laws would apply. Therefore discussions were also held with city and county police departments having jurisdiction where the equipment was located. Resolution as to jurisdiction came only after careful review of additional evidence and discussions with the law enforcement agencies on the range of laws being violated.

During review of the activity, Boeing investigators determined the intruders were using Boeing computing resources primarily to crack passwords. One very important password file the intruders moved to the Boeing system (in order to crack it), was found to belong to the United States District Court for the Western District of Washington located in Seattle, Washington. The intruders had successfully broken several passwords and gained access to the court's computer. It was primarily this fact that resulted in the FBI's jurisdiction in this case (felony violation of Title 18, USC Section 371, "Conspiracy to Defraud the United States Government").

The level of concern and the stakes were substantially raised once the intruders had shown interest in the federal court's computer. The information it contains is considered extremely sensitive and its compromise could have had very serious ramifications. If the intrusion had been confined to only one company's computing system, it is unclear if the case would have been considered serious enough for any prosecution to have taken place.

Finding the Culprits

At this point there was still no clue as to who the intruders were or where they might be operating from. The FBI asked the U.S. District judge for a court order to allow the placement of a pen trap on the Boeing telephone line to obtain the telephone number being used to access Boeing's systems. The proved to be more difficult than anticipated and resulted in an important lesson learned.

The unforeseen problem came as a result of Boeing's log-on message, presented any time a user is initializing access. The log-on banner notified users that it is a private computing system restricted to authorized individuals and that actual or attempted unauthorized use would result in criminal and civil prosecution. However, the banner failed to notify persons attempting access that the company reserved the right to review, monitor and record without notice or permission. Additionally, the log-on banner did not say that information obtained by such monitoring, review or recording was subject to review by law enforcement in connection with the investigation or prosecution of possible criminal activity on the system. In spite of this deficiency, the court allowed a trap to be placed. It is unknown if this would have proved damaging had the case gone to trial.

Nonetheless, those missing items in our log-on banner cost several days delay in obtaining the court order. Creating further delay was the fact that the phone company was unable to accommodate the request for a trap in a timely manner due to lack of resources. They were working higher priority cases, and because ours did not involve personal endangerment, we had to wait. After a week of waiting and applying pressure from all possible sources on the phone company, the trap was at last installed. Once it was in place, a telephone number was obtained and traced through telephone company records to a dormitory phone at a local university. At the same time, a recording device was installed that recorded the hackers' activity. Other than password cracking, their other main interest centered on reading the e-mail of Boeing system users. At this point it didn't take long

for the FBI through their investigative efforts to identify the two hackers.

Time to Close the Door

By this time over two weeks had gone by and the decision was made to go ahead "quietly" with the recovery part of our plan. Although we wanted to begin closing our door, we knew this could tip them off. In order to prove, without a doubt, who's hands and faces were behind the computer, it was imperative to catch the intruders in the act. We felt that even though the risk was low that every password had been cracked on Boeing's system, we decided to take no chances. We started by distributing a number of security software tools to system administrators and by asking them to reset all passwords on their systems. Consequently, our plan required us to ask system administrators to bring down production computer systems. This assured closing down the intruders' access. The administrators needed executive management's approval to bring down production systems for password resetting. To obtain this approval, we decided to have key executives in each division sign a letter authorizing our system administrators to follow designated instructions to bring down the systems. The letter also emphasized to administrators the extremely sensitive nature of the issue and they were advised not to discuss it with anyone. Here we learned another hard lesson.

These memos turned out to be a strategic error. While they were hand delivered to only a very few people, it took less than an hour before someone in the company faxed the letter to a local radio and TV station. Before the close of business, it had hit the local news. By early evening, national news agencies had begun to pick up the story. We felt fortunate that we had previously briefed our public relations executives so they were prepared to handle the situation.

Arrests and Indictments

The premature disclosure that someone was "breaking into Boeing's computers," forced Boeing and law enforcement to change their plans immediately. Obviously, our plan to synchronize the arrest with the FBI was compromised. Their agents were forced to switch quickly to plan "B." Arrests of the two hackers were made the following week, and a full confession was obtained. They were charged with a felony, "Conspiracy to Defraud the United States Government." As is typical in these cases, the hackers were initially quite proud of what they had done and consequently were more than happy to show how smart they had been. Both had prior records for theft of computer equipment.

In February 1993, the charges were plea bargained to a misdemeanor, violation of the "Computer Fraud and Abuse Act of 1986." In June 1993 the hackers were sentenced to 250 hours of community service, 5 years probation, and $30,000 in restitution ($28,000 to Boeing). Since the closing of this case, both individuals have been re-arrested for violation of parole for the theft of credit card numbers and cellular phone fraud.

In many ways our intruders were typical of nondestructive hackers. Their method of operation was to "network navigate" (a "hacker" term used to describe a game whose objective is to see how many computers they can access and browse through).

A call to openness and prevention

Traditionally the potential theft of competitive information has been the objective in providing a level of "due care." However, the integrity and availability of the information to legitimate users is also a major consideration in abating risk. Hackers who "network navigate," or browse, are of concern not only because they are stealing company time on computers, but because they may inadvertently compromise the "integrity" of the information. In some cases an unauthorized intruder can totally disable a computing or telephone system, consequently denying service for authorized users. This is not just a mere inconvenience. The real costs to the company are measured in terms of lost production and lost revenue.

As the technology and the automated business environment evolves, we see an alarming trend in which computer and communication system intrusions are the basis for criminal activities and/or monetary gain. There is a significant difference between the adolescent prankster and the criminal who has virtually unlimited access to corporate and government information. This change has happened so rapidly that many managers and corporate executives are unaware of the threat. It is especially difficult to quantify the threat in tangible terms because current statistics are unreliable, and in many cases, unavailable.

Just how bad is it out there?

At a recent conference of information technology security managers, the attendees were asked if their companies had been violated by hackers. Roughly one-third of the audience raised their hands. Secondly, about ten percent stated they had not, to their knowledge, been violated by hackers. Subsequently, the question was expanded to ask how many of their companies would not admit to whether or not they have been violated. The

much larger portion of the group indicated an affirmative answer to this question, demonstrating further the reluctance of many companies to disclose this type of information.

Unfortunately, as demonstrated above, some company management will not admit their systems have been violated. They often fear they are exposing corporate vulnerabilities of their own negligence in failing to exercise "due care." In addition, the specter of civil liability may preempt some corporations from notifying other victims who may be affected by the admitted penetration. Increasingly though, many companies are realizing that it is in their best interest to be conscientious and to view cooperative disclosure as being a "good business citizen."

The law in this area appears to have been set up primarily to protect government and government related industry, but not industry as a whole. This complicates the ability of private industry and legal authorities to adequately deal with these crimes. Tracking information technology crimes back to a human perpetrator in real-time is a challenge the legal community must address. Furthermore, we need people working on these cases who are both technically competent and able to present to lay jurors these technically complex cases in easily understood terms. With these challenges, industry and government must increase their training and support for improved security policy and tools.

The role of security education

Boeing began its computing security program back in the early '80s focusing on security for critical systems. During the last decade, increased emphasis has been placed on this program and now every computing system within Boeing is required to do an annual security self-assessment. This program has made great strides in the area of prevention and detection. But as we learned from this case, there are those whose determination can outwit the best of prevention and detection methods. Employee awareness is one of the strategic defenses against such attacks. In 1992, Boeing corporate computing board approved a plan requiring all users of company computers to attend an annual security awareness briefing. These briefings are designed to educate employees on the threat, what to look for, and their role in protecting our systems and information. The briefers also emphasize the importance of information security to our company's long-term competitiveness. We see our awareness activity as the cornerstone to a good security program.

In conclusion, government and private industry must begin communicating openly about the threat and sharing their experiences. The resulting synergy will only strengthen our ability to address these issues in the future and protect America's economy and technological advantage.

Have you heard about the

Center for Security Awareness Information?

The Department of Defense Security Institute (DoDSI) announces the 1 April 1995 inauguration of the Center for Security Awareness Information.

What exactly is this center all about?

The Center's mission is to involve the security community, both government agencies and industry, in sharing products and information to maintain and improve security awareness throughout the community. DoDSI will serve as the focal point for the center.

How do you get involved?

We ask that you submit for consideration security products or information that you or your company have developed. Our task is to make the security community aware of these products and ideas. If you know about an excellent product that you believe could or should be shared with the security community, tell us about it! We will follow-up. Through the mutual sharing of information and products, the whole security community benefits. Please get involved!

How is this going to be accomplished?

Security products referred to the DoDSI, will be reviewed and evaluated. We will then publish information about these products in the *Security Awareness Bulletin*, the *Quarterly Center for Security Awareness Information Report*, and other publications. Where appropriate, a point of contact for obtaining the product will be given. In some cases, DoDSI will provide products directly. Ultimately, we hope to provide some materials via the Internet as well as by paper copy.

What types of security products and information can you share?

We are interested in non-profit products for evaluation and broader distribution, however we will list commercial products separately in the quarterly report. Here are just a few examples of products and information you may consider submitting for review and evaluation: Videotapes, CAI/CBT software, computer games, computer graphics, computer slideshows, computer text files, films, information literature, job aids (paper products or software), manuals and handbooks, posters, print media inserts, promotional/miscellaneous items, quizzes and puzzles (paper or software), ready reference items, slide/tape sets, slides and slide sets, scripts and outlines, or services that your company is providing in the security field.

Is there a fee for submitting these products or information to the Center?

No, but we will ask each submitter, where appropriate, to sign a short release statement that gives us permission to reproduce and distribute the product.

Whom do we call to submit or discuss our security products and information?

Call Del Carrell, Manager of the Center, at (804) 279-5314 or DSN 695-5314. Or write her at:

Department of Defense Security Institute
Attn: Del Carrell
8000 Jefferson Davis Highway, Bldg. 33E
Richmond, VA 23297-5091

FROM DoDSI

New Independent Study Course

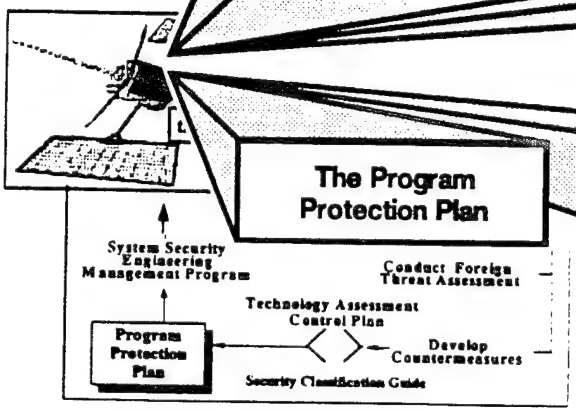
SUBCOURSE
DS 6100

EDITION
A

Department of Defense
Security Institute

Acquisition Systems Protection Background

Need for Program Protection Planning



The Program Protection Plan

Structure and General Responsibilities

Acquisition Systems Protection Program

Executive Overview

To enroll,
send DA Form 145 to:

Army Institute for
Professional Development
U.S. Army Training Support Center
Newport News, VA 23638-0001

There is NO CHARGE for DoDSI's independent study courses!

Army Correspondence Course Enrollment Application

DATE

For use of this form, see DA PAM 351-20: The proponent agency is TRADOC.

DATA REQUIRED BY THE PRIVACY ACT

AUTHORITY: 10 USC 3012 (B) and (G).
PRINCIPAL PURPOSE: To obtain information necessary by Army schools to administer student participation in the Army Correspondence Course Program.
ROUTINE USES: Used by Army schools to obtain basic data needed to determine eligibility for enrollment, process applications, maintain student records, and perform all other administrative functions inherent in student administration.
DISCLOSURE: Mandatory. Failure to provide this information could result in the applicant not being able to participate in the program.

*Submit one copy. See instructions on back page. Fill in all blocks (except **shaded blocks** which are for school use).*

1. Student SSN
2. Primary MOS/Duty MOS
3. CIV-SERIES
4. AOC Duty Position
5. ASI/SQI
6. Branch
7. DSN (Telephone) COMM (Telephone)
8. Group Number
9. Rank/Civ Grade
10. Component Code
11. RYE Date Day Month (abbreviate) Year
12. School Code
13. Enrollment Code
14. Phase
15. Course Number
16. Rep Qty
17. Unit Identification Code
18. Subcourse Exemption
19. I REQUEST ENROLLMENT IN: (Course Title, MOS if applicable or subcourses desired).
(Do not list individual subcourses if you are enrolling in a course).

NOTE: If you were previously enrolled in this course, indicate date of termination of enrollment. _____

Are you currently enrolled in the ACCP? _____ YES _____ NO

20. To: (School address, including ZIP Code)

The Army Institute for Professional Development
U.S. Army Training Support Center
Newport News, VA 23628-9989

THRU: (Unit to which assigned)

21. Title of approving official

Unit Address Line 1 Unit Designation (May not be left blank.)

Unit Address Line 2 P.O. Box or Street (May be left blank.)

Unit Address Line 3 City, Post or APO/FPO State or AE/AP/AA Zip + 4

FROM: (Mailing address to which subcourses are to be sent)

22. Last Name First Name Middle Initial

Student Address Line 1 Unit Designation or P.O. Box or Street (May not be left blank.)

Student Address Line 2 P.O. Box or Street (if not given on Student Address, Line 1)

Student Address Line 3 City, Post, or APO/FPO State or AE/AP/AA Zip + 4

23. **ARMY SCHOOL COURSES AND CORRESPONDENCE COURSES COMPLETED**

SCHOOL	TITLES OF RESIDENT OR NONRESIDENT COURSES OR INDIVIDUAL SUBCOURSES COMPLETED	DATES

The Commander will verify the above from personnel records or soldier's individual records.

24. I have reviewed DA PAM 351-20, and understand the eligibility requirements that I must maintain to sustain my enrollment in this course. I further understand that assistance is not authorized when completing subcourse test.

Signature of Applicant _____

25. I have reviewed the course objectives and prerequisite enrollment requirements in DA PAM 351-20 and determined the applicant is eligible for enrollment in this course.

Unit Cdr or other approving officer
Name (printed or typed) _____ Date _____

Signature _____

DA PAM 351-20 contains information pertaining to enrollment qualifications, submission of application and courses available.

INSTRUCTIONS TO APPLICANT

Complete by legibly printing only in areas that are **not shaded**. The shaded areas are used for data entry. Enter only one character per block (example below).

1. Student SSN

2	4	4	3	2	0	1	6	4

9. Rank/Civ Grade

S	G	T	M	A	J

ITEM 1. SSN Foreign students must leave blank.

ITEM 2. Student's PMOS (Primary MOS) and DMOS (Duty MOS). Enter numeric and alpha identifiers.

ITEM 3. Civ-Series number (for example 1702).

ITEM 4. AOC Area of Concentration or Duty Position. Submit information required to qualify for enrollment.

ITEM 9. RANK: RA warrant officers and enlisted personnel who hold a reserve commission and are enrolling in officer career development courses must enroll in their reserve capacity.

ITEM 10. Component Code: Student categories: Enter one of the following as appropriate:

02	Active Duty	09	USAR ENL	15	FGN CIV	20	CADET
03	RA/AUS ENL	10	NGUS ENL	16	USAF	31	IRR (OFF)
06	RET MILITARY	12	NDCC/ROTC/JR	17	USN	32	IRR (ENL)
07	USAR OFF/WO	13	FGN MIL	18	USCG	33	NAF (VOL)
08	NGUS OFF/WO	14	U.S. CIV	19	USMC		

ITEM 11 RYE Date (Retirement Year Ending Date): USAR and NG applicants not on active duty must enter the anniversary date of their retirement year ending day and month.

Where to mail application:

SCHOOL MAILING ADDRESS: Please check DA PAM 351-20 for appropriate address of school with whom you are seeking enrollment, e.g., Academy of Health Science, The Judge Advocate General's School, Army Logistics Management College, the Army Institute for Professional Development, etc.

REVERSE OF DA FORM 145

A New Point of Contact for Security Professionals

introducing the .....

Center for Information Systems Security (CISS)

5113 Leesburg Pike, Suite 400
Falls Church, Virginia 22041-3230
Phone number: (703) 756-7960, DSN 289-7960
Fax: (703) 756-7949

Goal

The CISS goal is to create and manage a unified, fully integrated information systems security program for all Defense Information Infrastructure (DII) systems.

Mission

CISS is a focal point for assuring availability, integrity and confidentiality of DII Automated Information Systems (AIS) information. The Center has the responsibility to provide a unified information systems security policy and architecture for all DII information systems. CISS also supports policy and architecture implementation, and provides direct Information Systems Security (INFOSEC) support to DII programs. A key effort for CISS is to define requirements for DII INFOSEC standards and protocols. CISS also expedites Multilevel Security (MLS) implementation, and provides central coordination and reporting for response to all DoD INFOSEC incidents.

Scope

The scope of operations for the Center for Information Systems Security includes:

- Execution of the Defense Information Systems Security Program (DISSP) missions and functions,
- Execution of the DoD MLS mission,
- Support to the Assistant Secretary of Defense/Command, Control, Communications, and Intelligence (ASD/C3I).

Background

CISS is a Joint DISA/NSA organization charged to execute centrally managed INFOSEC functions within the DoD. Starting in 1990 as the Defense Information Systems Security Program (DISSP), this organization was elevated to a new Center within the DISA under the Joint Interoperability and Engineering Organization (JIEO). CISS executes DISSP, MLS, and other DISA missions and functions. The CISS Director, Mr. Robert Ayers, is the Director of DISSP, and COL John Sheldon serves as the Program Manager of the MLS Program. This increase in organizational posture highlights the expanded importance of INFOSEC in the DoD.

Directorates & Functions

INFOSEC Policy, Plans, & Programs

- Provides recommendations to ASD/C3I concerning DoD INFOSEC program fiscal review, program monitoring, and program prioritization.
- Manages the government-wide INFOSEC Omnibus Contract.
- Prepares economic and cost analyses and business cases associated with Center and DoD INFOSEC.
- Supports ASD/C3I in developing INFOSEC policy, directives, and regulations for DoD.
- Develops and maintains a comprehensive INFOSEC awareness program.

Architecture and Engineering Directorate

- Ensures DII programs implement DoD Goal Security Architecture.
- Develops security architectures for the DII.
- Develops INFOSEC transition plans for DII implementation.
- Performs configuration management of DII architecture.
- Recommends INFOSEC AIS/Technology standards.
- Maintains the DoD Goal Security Architecture

Evaluation, Certification, and Accreditation Directorate

- Creates a focal point in DoD for life cycle security support for major automated information systems, These systems include the DoD business mission area, the Defense Message System (DMS), and other critical information systems that support the DII.
- Develops, implements, and manages uniform security certification and accreditation procedures for classified and unclassified DoD information systems.
- Performs security certification of DoD Mega-Data Centers.
- Establishes a program to ensure DoD Information Systems are operated and maintained in accordance with their accreditation.

Security Products Program Directorate

- Maintains a database of INFOSEC products and requirements.
- Consolidates defense community INFOSEC product requirements and needs.
- Ensures the application of INFOSEC products and services to DoD Information Systems' programs.
- Maintains technology transfer program with government and industry.

Professionalization Directorate

- Incorporates customer requirements into the INFOSEC Professionalization Program.
- Develops and coordinates an INFOSEC professional career development program for DoD.
- Standardizes execution of INFOSEC education and training throughout the DoD.

Multilevel Security Directorate

- Plans and coordinate DoD MLS projects and initiatives.
- Assesses MLS products and technology for use in DoD information systems.
- Supports fielding and implementation of MLS capabilities at high-priority commands.
- Identifies MLS technology and product requirements.
- Provides a set of MLS solutions for widespread deployment. Examples include:
- Operations/Intelligence Interface,
- Two-level Workstations,
- Worldwide Military Command and Control System (WWMCCS) Guard,
- Releasibility Guard (under development),
- Secure E-mail Guard (under development).

INFOSEC Countermeasures Directorate

- Establishes a program to develop and incorporate INFOSEC countermeasures into the DII.
- Conducts a Vulnerabilities Analysis and Assistance Program (VAAP) for DoD AISs.
- Disseminates threat information provided by the intelligence community to DoD elements.
- Operates an Automated Information Systems Security Incident Support Team (ASSIST).

ASSIST Program

ASSIST is the action arm of the DoD responding to INFOSEC incidents worldwide, 24 hours a day. ASSIST can be reached during normal business hours at (703) 756-7974, DSN 289-7974; or at any time of day by dialing 1-800-SKY-PAGE or (800) 759-7243; and entering PIN 2133937. Follow the prompts and enter the call back number. If immediate assistance is needed, preface the call back number with 999, and the duty officer will call back within 5 minutes.

Subscriptions to DISSPATCH, the Center for Information Systems Security's INFOSEC newsletter, may be ordered by faxing a request to the attention of "Newsletter/TGA" at fax (703) 756-7949, or by calling (703) 756-7944, DSN 289-7944.

Advanced Industrial Security Management Course Hits the Road!

DoDSI recently presented the Advanced Industrial Security Management Course in Reston, Virginia, at the LOGICON Inc. facility. The responses from the attendees were extremely complimentary, due in large part to our host LOGICON. The classrooms they provided (as well as the coffee) greatly added to the success of the course. We'd like to thank Diane, Marcie, and Dora for all their help.

We plan on offering the AISMC in the field next fiscal year. If your company would be interested in sponsoring it at one of your facilities, please call Paul McCray on (804) 279-4759.

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your **address label**

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

- ❑ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.
- ❑ **Announcement of Products and Resources**. March 1996. A catalog of security education videos, publications, posters, and more you can order.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. April 1995.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment. May 1995.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.
- ❑ **Take A Security Break.** Questions and answers on security and other topics.
- ❑ **Take Another Security Break.** More questions and answers.
- ❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)**
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)**
- ❑ Regional Cooperation for Security Education **(1-91)**
- ❑ AIS Security **(2-91)**
- ❑ Economic Espionage **(1-92)**
- ❑ OPSEC **(3-92)**
- ❑ What is the Threat and the New Strategy? **(4-92)**
- ❑ Acquisition Systems Protection **(1-93)**
- ❑ Treaty Inspections and Security **(2-93)**
- ❑ Research on Espionage **(1-94)**
- ❑ Information Systems Security **(2-94)**
- ❑ Acquisition Systems Protection Program **(3-94)**
- ❑ Aldrich H. Ames Espionage Case **(4-94)**
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
- ❑ The Threat to U.S. Technology **(2-95)**
- ❑ Entering a New Era in Security **(1-96)**